Systems Management

Component Architecture

Revision Date: January 15, 2002

Table of Contents

Section 1 - Background and Decision Tools

Business Direction

Business Direction, which includes Business Influences, Goals and Objectives, forms the foundation of the BEAM process and the DMV's Enterprise Architecture. This foundation is the first step from which all information technology decisions are made and can be traced. Business objectives are common across the DMV enterprise and represent DMV's stated direction for fulfilling the organization's mission. The primary objective of the BEAM process is to develop a flexible, comprehensive, maintainable framework to manage the rapid evolution of technologies that support the business directions of the DMV. This approach will directly link all technologies implemented to specific DMV goals and/or objectives.

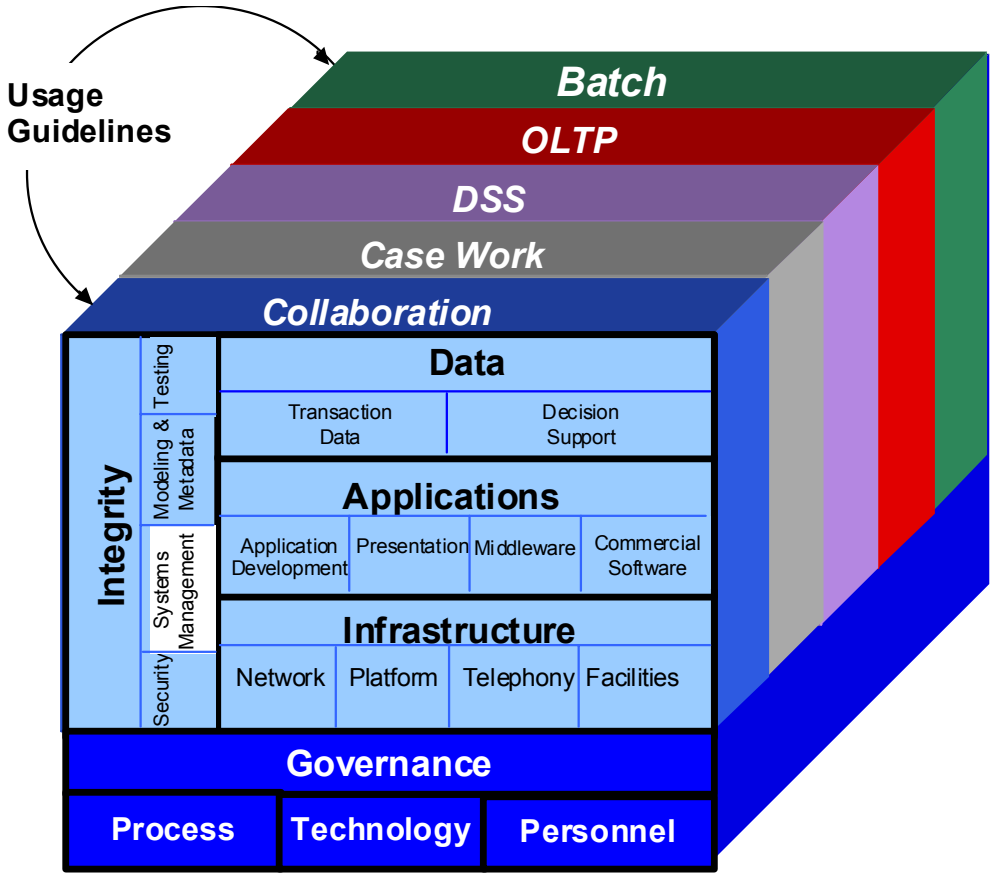
Architecture Requirements

The Architecture Requirements consists of two sections, Information Requirements and Technology Requirements. This is the first step in the BEAM process that begins to focus on specific technologies.

Information Requirements represent the informational needs that are necessary to fulfill DMV's Business Goals and Objectives. Information Requirements bridge the gap between what the Business Goals and Objectives are and what DMV's information systems must deliver to allow management to met these goals and objectives. An individual Information Requirement is typically applicable to more than one Business Objective. Information Requirements are not system or division specific, rather they are related to the information itself. Information delivery refers to the process of delivering information to and from people or groups of people, rather than the input or output of data from databases or applications.

Technology Requirements represent the technologies that satisfy the Information Requirements. In addition, the Technology Requirements feed the DMV Domain Model (Figure 1) which organizes each IT technology into manageable categories called domains, components and Sub-Components. The Technology Requirements detail the specific technologies that satisfy the Information Requirements.

Figure 1 - Domains and Components



Conceptual Architecture

The Conceptual Architecture defines the principles and industry-leading best practices that will guide future IT and process decisions. The Conceptual Architecture is derived from DMV's Business Goals, Objectives, Information Requirements and Technology Requirements. Conceptual Architecture Principles (CAPs) are important to the BEAM process because they help ensure that the decisions made later in the Component Architecture development process are consistent.

The following pages contain CAPs for the Systems Management Component:

Applicable Conceptual Architecture Principles (CAPs)	
Gov-Proc 6	Follow a total cost of ownership (TCO) methodology.
Gov-Proc 7	Develop service level agreements (SLA) for all IT services.
Gov Proc 12	DMV must leverage the BEAM Usage Guidelines when developing and implementing IT systems.
Gov-Tech 1	Design systems (i.e., hardware, software, operating systems, networks) to be robust enough to handle changing business needs.
Gov-Tech 2	Deploy information systems across an N-Tier*, distributed computing environment.
Gov-Tech 3	Design flexibility into the architecture to accommodate continuing business changes and improvements in technology.
Gov-Tech 4	Design DMV systems for scalability and increased functionality.
Gov-Tech 5	Invest in industry leading vendors, best practices, technology standards and products
Intra 1	Centrally manage DMV's IT infrastructure.
Infra 2	Employ communications protocols that span multiple platforms and diverse operating systems.
Infra 3	Regardless of where an employee connects to the infrastructure, once authenticated, provide access to all system resources.
Infra 4	Manage the transport infrastructure, desktop systems and servers with a responsive, measurable set of service level objectives.
Infra 5	Provide an effective integration of DMV's automated voice processing tools and IT systems.
Infra 6	Supporting facilities and services must be engineered and managed to ensure that DMV can respond to new business requirements.
Integrity 1	Centrally manage IT security.
Integrity 2	Ensure that all data stored on servers will be backed-up and recoverable.
Integrity 3	Conduct business without putting the security of DMV's data and information at risk.
Integrity 4	Design for a "single sign-on" user authentication process.
Integrity 5	Design for centralized management of user authorizations for all applications and enterprise services.
Integrity 6	Support a Disaster Recovery Plan that allows resumption of critical processes.

* For a definition of an N-Tier environment, please see the Glossary section of the BEAM intranet site at: http://dmvweb/isd/beam/

Section 2 - BEAM Recommendations

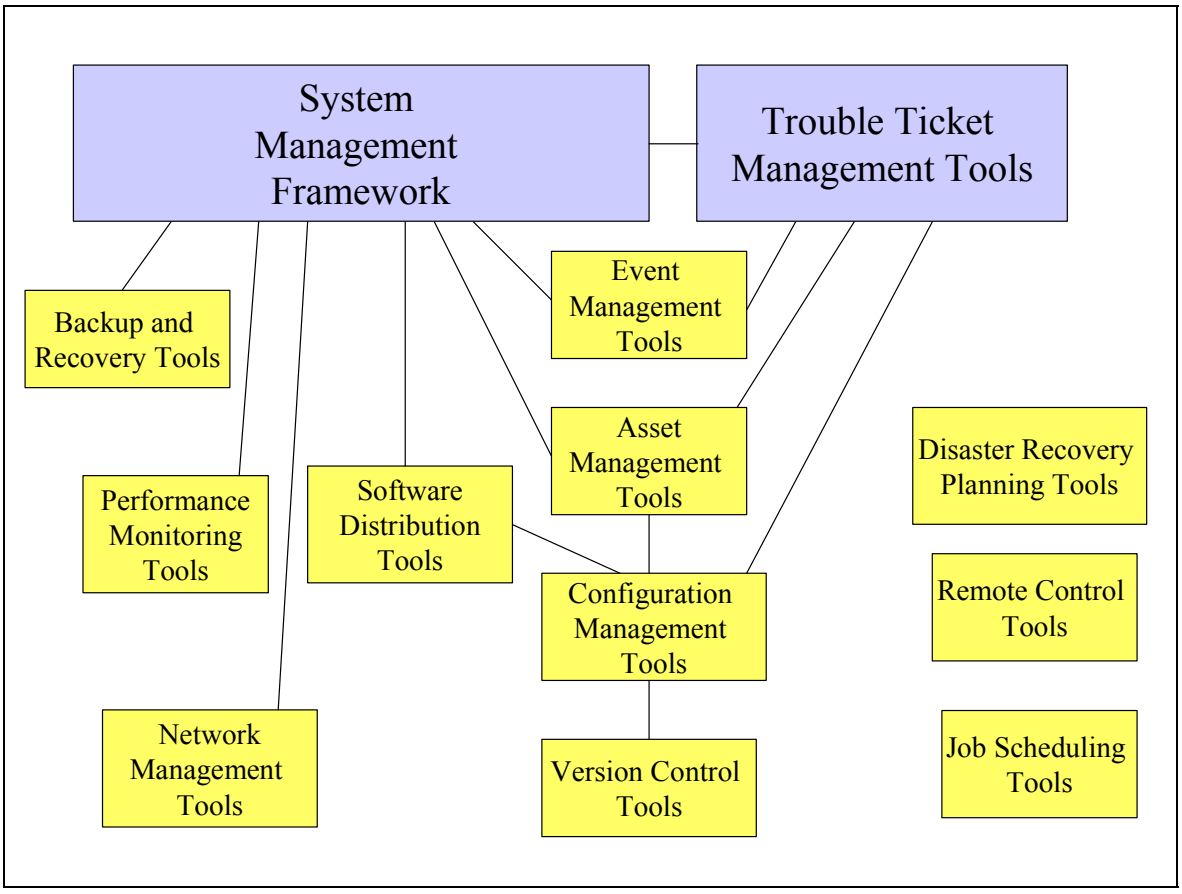
Systems Management Component

The Systems Management Component is DMV's framework that identifies the requirements for managing and supporting the IT environment with primary emphasis on centrally managing distributed systems. Resources managed include the computing platforms, security, databases, applications, networks, Intranet, and Internet components necessary to conduct DMV's automated business functions. The systems management component is divided into a number of Sub-Components based upon a logical and/or physical breakdown. The Sub-Components will help facilitate the development of the systems management component by partitioning the technology categories into smaller more manageable pieces.

The Sub-Components are further broken down into the following categories:

- Systems Management Frameworks Sub-Component
- Asset Management Tools Sub-Component
- Event Management Tools Sub-Component
- Trouble Ticket Management Tools Sub-Component
- Configuration Management Tools Sub-Component
- Remote Control Tools Sub-Component
- Software Distribution Tools Sub-Component
- Job Scheduling Tools Sub-Component
- Network Management Tools Sub-Component
- Performance Monitoring Tools Sub-Component
- Backup and Recovery Tools Sub-Component
- Disaster Recovery Sub-Component
- Version Control Tools Sub-Component

Figure 2: System Management Sub-Component Relationships



Systems Management Component Principles

Statements agreed to by the DMV technology professionals that direct the selection, acquisition, deployment and management of the Systems Management Component.

#	Systems Management Component Principles
1	Systems management decisions must support business objectives.
2	Invest in system infrastructure based not only on short-term considerations, but when it provides long-term support cost savings utilizing total cost of ownership (TCO) analysis.
3	Design systems to support remote monitoring and management to provide reliable and highly available services for network servers, desktop equipment and data center sites.
4	Utilize an enterprise asset system to manage hardware, software, asset financial statuss, and inventories.
5	Both Business and IT must proactively manage disk space, network bandwidth and other system resources to provide agreed, achievable, affordable services, supported by cost-benefit analysis when feasible.
6	Actively monitor system resources to identify and correct: • potential space problems • locking issues • system errors • spinning processes • excessive CPU consumption • erred batch jobs,etc. NOTE: *Please see the Security component for details of additional system events which must be monitored.*
8	Utilize a standard error logging process which is incorporated within a formalized escalation process. Defect reporting must be incorporated as part of this process in order to ensure that any faults and defects are identified and that corrective action is being taken.
9	A central point of control should be used for monitoring all application systems, network devices and network links in order to manage and optimize performance.
10	Establish a DMV management-approved method of identifying all components of a configuration, from the start of the system development lifecycle
11	Implement audit procedures to verify physical locations of hardware, software and documentation and to confirm adherence to DMV documented practices
12	Audit systems management tools, methodologies and processes periodically to verify standards compliance and satisfaction of business requirements.
13	Implement a Change Management process to plan, implement, monitor, control and report/record configuration changes across the development lifecycle, to ensure that service levels are not impaired by change activity.

#	
14	Deploy systems management tools that can support an object-oriented approach.
15	Select systems management tools that can operate within an industry standard distributed systems management framework (including help desk software).
16	Manage network traffic in accordance with approved policies and defined events
17	Design networks and network administrative processes to maximize the opportunity for remote management
18	Buy commercial systems management tools rather than developing tools within DMV
19	When systems management tools have a presentation layer, ensure that selected tools comply with n-tier architecture as defined in BEAM
20	Trouble ticket tools must provide the user with a single point of contact for reporting and tracking all DMV system issues

System Management Sub-Components

Systems Management Framework Sub-Component

The Systems management frameworks are enterprise platforms designed to encompass end-to-end management of application inventory, performance and monitoring; network device monitoring, performance and capacity planning; software distribution and control; and overall administration of the IT environment. Typically, network/systems management frameworks provide "hooks" to specialized applications for a given part of enterprise network/systems management such as help desk, LAN management, storage management, etc.

Justification

- Secures and monitors sensitive information
- Easy control and management of technology resources
- Manages total cost of ownership

Standards

#	Systems Management Frameworks Standards
1.	Select a Systems Management Framework that supports Desktop Management Interface (DMI). **Description:** DMI is a set of Application Programming Interfaces (APIs) that allow software to gather information about a computer environment. DMI is platform and operating system independent. DMI was developed by the Desktop Management Task Force, a consortium of hardware manufacturers. http://www.dmtf.org **Rationale:** • Use of DMI-compliant software makes use of an industry-standard, non-vendor-specific framework for desktop management, reducing the likelihood of proprietary lock-in.
2.	The Systems Management Framework must be able to interface with the DMV standard Trouble Ticket system. **Rationale:** • The Trouble Ticket system requires visibility into the status of current system events, in order

#	
	to support user queries; the System Management Framework should automatically submit some categories of events directly to the Trouble Ticket system.

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the selection of the appropriate product for your environment.

#	Systems Management Framework—Products
1.	HP OpenView **Rationale:** • Supports DMI • Can integrate with DMV Standard trouble Ticket system via Remedy Link for HP OpenView Network Node Manager • Operates on Solaris, AIX, HP/UX, Windows NT and Windows 2000 • Already in use at DMV
2.	Oracle Enterprise Manager **Rationale:** • Supports management of Oracle RDBMS and applications • Already in use at DMV
3.	IBM NetView **Rationale:** • Framework for SNA-based OS/390 systems • Already in use on DMV systems at Teale Data Center

Tech Watch

- System Management tools for OS/390 systems
- OS/390 application-layer monitoring tools (CAMVDCS?)
- Java Management Interface for J2EE applications
- Further Rededy/OpenView integrations
- Integrated management frameworks for Oracle, DB2 and SQL Server

Review Cycle

6 Months

Asset Management Tools Sub-Component

Asset management encompasses the monitoring, tracking and accounting of the IT environment. This includes accounting for all hardware and software accessible to the network. This may also include software metering, which tracks the number of floating licenses being used at any particular time for an organization's software packages.

Examples: SMS

Justification

- Enables accurate inventory count
- Allows for proper dissemination of inventory information and reporting
- Secures and monitors sensitive information
- Enables better accounting, budgeting, contract management and maintenance

Standards

#	Asset Management Tools Standards
1.	Asset Management Tools must be able to interface with System Management Framework (where such tools exist) **Rationale:** • The Asset Management Tools must be able to interface with the DMV standard Systems Management Framework, in order to facilitate centralized control of system assets. NOTE: It is understood that some asset management tools (for example, for physical asset inventory) cannot comply with this standard.
2.	Network-based Asset Management Tools must comply with the Systems Management Services (SMS) API. **Rationale:** • The Asset Management Tools must be able to interface with the DMV standard Systems Management Services API, in order to integrate effectively with other DMV Systems Management tools. NOTE: It is understood that some asset management tools (for example, for physical asset inventory) cannot currently comply with this standard.
3.	Asset Management tools must be able to interface with the DMV standard Trouble Ticket system. **Rationale:** • The Trouble Ticket system requires visibility into data generated by the Asset Management tools.

#	Asset Management Tools Standards
4.	Asset Management tools must be able to interface with the DMV standard Configuration Management system. **Rationale:** • Asset Management tools can be used to verify the completion of change requests; it should be possible to capture this verification data without the need to re-enter data.
5.	Online Asset Management tools must support software metering. **Rationale:** • Management of floating licenses is a critical DMV support function; Asset Management tools must be available to enable this function.

Products

#	Asset Management Framework-- Products
1.	Rededy Asset Management **Rationale:** • Integrates with DMV standard System Management Framework (though third-party tools are required) • Already in use at DMV

Tech Watch

- Integration between OpenView and DMV CM products
- Asset management integration between OS/390 and other DMV platforms/operating systems

Review Cycle

- 6 Months

Event Management Tools Sub-Component

Event management technologies and tools focus on the monitoring, management and interpretation of various network and system events through the use of intelligent agents. Intelligent agents generate events when thresholds are exceeded or events fail. The two approaches to event management include:

- Filtering and forwarding
- Event correlation

Justification

- Ensures computers are run optimally
- Ensures availability of all computers on the network
- Secures and monitors sensitive information
- Ensures applications do not run out of necessary resources

Standards

#	Event Management Tools Standards
1.	Select Event Management Tools that are able to interface with the DMV standard System Management Framework **Rationale:** • The Event Management Tools must be able to interface with the DMV standard Systems Management Framework, since centralized control cannot be effective without centralized monitoring.
2.	Select tools that perform both filtering and forwarding, and event correlation. **Rationale:** • The Event Management Tools must be able to interface with the DMV standard Systems Management Framework, since centralized control cannot be effective without centralized monitoring.
3.	Event Management tools must be able to interface (either directly or indirectly) with the DMV standard Trouble Ticket system. **Rationale:** • Some categories of events should cause the automatic generation of trouble tickets; help desks require visibility into the current system events when investigating some trouble reports.
4.	Event Management tools for TCP/IP-based systems must provide support for SNMP.

#	
	Rationale: • SNMP is a standard protocol for event reporting over TCP/IP networks.

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the research and selection process for the department.

#	Event Management Framework Products
1.	HP OpenView Network Node Manager Application **Rationale:** • Able to interface with OpenView framework • Supports SNMP • Supports RMON • Provides event filtering • Already in use at DMV
2.	HP OpenView Event Correlation Services for Network Node Manager **Rationale:** • Able to interface with OpenView framework • Provides event correlation
3.	California Motor Vehicles Data Communication System (CAMVDCS) **Rationale:** • Event management for OS/390 platform
4.	Oracle Enterprise Manager **Rationale:** • Able to interface with OpenView framework • Supports management event of Oracle RDBMS and applications • In use at DMV

Tech Watch

- Event management for OS/390
- Event management integration between OS/390 and other DMV platforms/operating systems
- Integrated event management tool for Oracle, DB2 and SQL Server

Review Cycle

- 6 Months

Trouble Ticket Management Sub-Component

Trouble ticket software provides the means to log in problems and track them until solved. It also provides the management information regarding support activities.

This is a technology that also applies to Application Development.

Justification

- Facilitates IT support activities
- Increased response time for end users with IT problems
- Improved management of trouble tickets

Standards

#	Trouble Ticket Management Tools Standards
1.	Trouble Ticket Management Tools must be able to interface with DMV Configuration Management Standards **Rationale:** • The trouble ticket management tool must be able to interface with the DMV standard Configuration Management tools, since trouble tickets that lead to system changes must be cross-referenced to change requests.
2.	Trouble Ticket Management tools must be able to interface with the DMV standard Asset Management tools. **Rationale:** • The Trouble Ticket system requires visibility into data generated by the Asset Management tools.
3.	Trouble Ticket Tools must interface with DMV Time Management systems. **Rationale:** • The Trouble Ticket system tracks time spent on resolving tickets. This prevents duplication of data entry between the two systems.

Products

#	Trouble Ticket Management Products
1.	Remedy **Rationale:** • Can inter-operate with OpenView Asset Management via XML • Already in use at DMV

Tech Watch

- Remedy/Endevor integration tools:
  - www.toucantech.com
  - Polaris Technologies Help Desk Integration Kit for Remedy and Harvest
- Migration of PITS to Remedy
- Migration of AFSR Trouble Ticket System to Remedy

Review Cycle

- 6 Months

Configuration Management Sub-Component

Configuration management technology and tools allow for the monitoring, management and control of enterprise network and application configurations, from an administrative perspective. Configuration management tools can either be utilized specifically as a function built in an enterprise network/systems management framework, or integrated with other element management tools as a component of the enterprise network/systems management process.

This is a technology that also applies to Application Development.

Justification

- Lowers the total cost of ownership (TCO) for desktop and notebook computers
- Helps reduce the support burden
- Facilitates easier administration of large fleets of desktop and mobile computers
- Increases desktop troubleshooting capabilities and effectiveness

Standards

#	Configuration Management Tools Standards
1.	Configuration Management Tools must support compliance with the DMV ISD Software Configuration Management Planning (SCM) Process. **Rationale:** • In order to be effective in meeting DMV's needs, any CM tool must provide artifacts and workflow to support the defined DMV process.
2.	Configuration Management Tools must be able to interface with the DMV Version Control Standard **Rationale:** • The Configuration Management tool must be able to interface with the version control tools on the applicable platforms. Otherwise, it will not be possible to automatically associate specific system changes with the reasons for change.
3.	Configuration Management Tools must be able to interface with the DMV Trouble Ticket Tools Standard **Rationale:** • The Configuration Management tool must be able to interface with the DMV trouble-ticket tool on the applicable platforms. Otherwise, it will not be possible to automatically associate change

#	
	requests with trouble tickets, and it will not be possible to automatically determine the status of trouble tickets whose resolution requires system changes.

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the selection of the appropriate product for your environment.

#	Configuration Management Tools Products
1.	HP OpenView **Rationale:** • For configuration reporting and configuration auditing on distributed platforms and operating systems • In use at DMV.
2.	Endevor **Rationale:** • For configuration identification and configuration control on OS/390 • In use at DMV.

Tech Watch

- Endevor Webstation to provide a Web-based interface for Endevor on OS/390
- (Longer-term) IBM System Life Cycle Manaqgement for OS/390-based solution to replace Endevor: http://www.ibmlink.ibm.com/usalets&parms=H_200-405
- Convergence of Configuration Management with Software Distribution Tools
- Investigate:
  - Remedy Change Management
  - CGI Group
  - Rational ClearQuest
  - Chicago Interface (for OS/390)

Review Cycle

- 6 Months

Remote Control Sub-Component

Software that allows a user at a local computer to have control of a remote computer via modem. The software must be installed on both computers, which then allows both users to run the remote computer and see the same screen. Remote control operation is used to take control of an unattended desktop personal computer from a remote location as well as to provide instruction and technical support to remote users.

Justification

- Lowers the total cost of ownership (TCO) for desktop and notebook computers
- Helps reduce the support burden
- Facilitates easier administration of large fleets of desktop and mobile computers
- Increases desktop troubleshooting capabilities and effectiveness

Standards

#	Remote Control Tools Standards
1.	Select an industry-standard, “best of breed” Remote Control Tool. **Rationale:** • Remote Control tools represent point solutions, with minimum opportunity for integration with other DMV Systems Management tools. Therefore, vendor viability and tool performance are the primary selection criteria.
2.	The Remote Control Tool must give the user positive indication that the tool is in use. **Rationale:** • Use of remote control tools when confidential data is being processed can compromise the security of the data. Therefore, users must be able to verify that a remote control tool is not in use when handling such data.
3.	Utilize strong authentication when using Remote Control Tools. **Rationale:** • Use of remote control tools when confidential data is being processed can compromise the security of the data. Use of strong authentication helps to ensure the protection of this data, and enables auditing of access.
4.	Vendors must comply with DMV Security and Remote Control Tools standards when accessing DMV systems for maintenance or upgrades. **Rationale:**

#	
	• In order to preserve confidentiality, protection of DMV data by external vendors must be at least as strong as that within DMV.

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the selection of the appropriate product for your environment.

#	Remote Control Tools Products
1.	Timbuktu Pro Enterprise Edition **Rationale:** • Provides clients with notification when connecting • Contains additional security features not found in Timbuktu Pro Workstation • Supports MacOS and Windows platforms • In use at DMV
2.	Netfinity Service Manager **Rationale:** • Exception for platforms running Netfinity, since Timbuktu and Netfinity cannot inter-operate • In use at DMV

Tech Watch

- Remote-control facilities are part of Windows XP—may eventually replace third-party remote-control tools

Review Cycle

- 6 Months

Software Distribution Tools Sub-Component

Software distribution technologies and tools focus on the rapid deployment and synchronization of mission-critical or desktop applications to multiple locations from a central point. Software distribution and change management tools can either be utilized specifically as a function built in an enterprise network/systems management framework, or integrated with other element management tools as a component of the enterprise network/systems management process.

Justification

- Reduces the complexity of the application system release process
- Lowers the total cost of ownership (TCO)
- Eases the burden of user involvement in the application set-up and installation process
- Enables faster and more efficient delivery of business solutions

Standards

#	Software Distribution Tools Standards
1.	Software Distribution Tools must be able to interface with System Management Framework **Rationale:** • The Software Distribution Tools must be able to interface with the DMV standard Systems Management Framework, in order to integrate centralized monitoring of installed software with its distribution.
2.	Software Distribution Tools must be able to interface with the DMV standard Configuration Management tools. **Rationale:** • The Software Distribution Tools must be able to interface with the DMV standard Configuration Management tools, in order to enable proper change control of program and/or system modifications, fixes and upgrades.
3.	Software Distribution Tools must be compliant with DMV Security standards. **Rationale:** • The Software Distribution Tools must be able to interface with the DMV Security standards, since changes to DMV systems can potentially compromise DMV security and system availability.

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the selection of the appropriate product for your environment.

#	Software Distribution Tools Products
1.	Cisco Management Tools **Rationale:** • Supports Cisco routers and other Cisco products • In use at DMV
2.	Microsoft Systems Management Server (SMS) **Rationale:** • Supports Windows NT and Windows 2000 platforms • Able to interface with DMV standard System Management Framework (OpenView) • In use at DMV (for desktops only) • Please note Tech Watch below regarding Novadyne
3.	Tivoli NetView/DM for AIX **Rationale:** • Supports AIX platforms • In use at DMV
4.	Endevor **Rationale:** • For use on mainframe platforms • In use at DMV

Tech Watch

- Distribution tools for HP-UX and Solaris platforms
- HP OpenView -compatible distribution tools for AIX
- Windows XP Auto-update feature—conformity with Standards 3 and 4?
- Novadyne as platform-independent replacement for Microsoft SMS
- Distribution tool for Mac platforms
- Automated software migration tools for Client/Server, Natural and RS6000 applications

Review Cycle

- 6 months

Job Scheduling Tools Sub-Component

Job scheduling tools are used to manage the scheduling, coordination and logging of batch jobs in a distributed environment. This allows synchronization of batch processing among multiple systems, and coordination of processing on distributed systems with mainframe processing.

Note that Component Principle 8 calls for centralized monitoring and control. Job scheduling tools should support this principle. Also please note that the subcomponent standards apply equally to off-the-shelf and DMV-developed solutions, for all platforms, including the native OS/390 environment.

Standards

#	Job Scheduling Tools Standards
1.	Require strong authentication when scheduling jobs. **Rationale:** • Control of software on DMV systems can potentially compromise system security and availability; therefore, its use must be restricted to authorized personnel.
2.	Job scheduling tools must provide a logging capability, based on user roles, to support auditing. **Rationale:** • It is necessary, in the DMV environment, to implement systems in a way that enhances accountability and ensures that it is possible to verify that required actions have been taken.

Products

#	Job Scheduling Tools Products
1.	Cybermation ESP Espresso **Rationale:** • Supports Windows NT, Windows 2000, AIX, Solaris, HP-UX and OS/390 Unix Services (requires Java Runtime 1.3) • In use at DMV (on mainframe only) • (NOTE) Was formerly called ESP Job Scheduler

Tech Watch

- Strong authentication for job scheduling tools

- Assess feasibility of migrating cron jobs on UNIX to Espresso, to achieve a common scheduling interface for both UNIX and mainframe.

Review Cycle

- 6 Months

Network Management Tools Sub-Component

Refers to the broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including:

- Security: Ensuring that the network is protected from unauthorized users
- Performance: Eliminating bottlenecks in the network
- Reliability: Making sure the network is available to users and responding to hardware and software malfunctions

Network management tools are usually integrated with distributed systems management frameworks.

Justification

- Ensures availability of all computers on the network
- Easy control and management of network resources
- Ensures availability and reliability of critical networks and supporting hardware
- Critical for disaster recovery and business resumption operations

Standards

#	Network Management Tools Standards
1.	On TCP/IP networks, select devices and software that support SNMP **Description:** Simple Network Management Protocol (SNMP) is a protocol for management of networks. While its usage is most commonly on TCP/IP networks, it is also possible to use SNMP on other networks. SNMP sends messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters. There are two versions of the SNMP protocol. SNMP version 1 is in wide use. SNMP2 has not been finalized, but some of its functionality has been provided by another technology called RMON. The primary definition of SNMP is in Internet Engineering Task Force (IETF) Request for Comment (RFC) 1157. **Rationale:**

#	
	• Use of SNMP enables industry-standard centralized network monitoring and control.
2.	On TCP/IP networks, where possible, select devices and software that support RMON **Description:** RMON (Remote Monitoring) protocol augments SNMP by adding nine further Management Information Bases (MIBs) to provide additional data on network usage. RMON is focused primarily on the MAC (Media Access Control) layer of the Operating Systems Interconnection (OSI) model. If RMON is to be used, network devices (such as switches and hubs) must be selected to support it. **Rationale:** • Use of RMON enables centralized network monitoring and control at a finer granularity than that provided solely by SNMP.
3.	Select Network Monitoring Tools that are able to interface with the DMV standard System Management Framework **Rationale:** • Network management tools should operate within the DMV standard systems management framework, in order to facilitate centralized management while requiring the minimum number of different tools and skill sets, and maximizing the possibility of integration with other tools.
4.	Network Monitoring Tools must enable the enforcement of fine-granularity access control when granting administrative access to the network. **Rationale:** • Allowing admin privileges to be restricted by domain or sub-domain reduces the likelihood of inadvertent or intentional actions by administrators that can compromise network availability.
5.	On SNA networks, select Network Monitoring Tools that support Systems Management component principles regarding security, performance and reliability. **Rationale:** • SNA network monitoring is a cooperative effort between DMV and Teale Data Center. Since these capabilities are not fully under DMV control, DMV should encourage the use of tools that will meet DMV's business needs.

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the selection of the appropriate product for your environment.

#	Network Management Tools Products
1.	HP OpenView **Rationale:** • For TCP/IP-based networks • Supports SNMP and RMON • Compatible with DMV standard System Management Framework (also OpenView) • In use at DMV
2.	Cisco Works **Rationale:** • Provides added functionality to support Cisco hardware • Supports SNMP and RMON • Compatible with DMV standard System Management Framework (OpenView) • In use at DMV
3.	Concord eHealth Suite **Rationale:** • For TCP/IP-based networks; supplements OpenView • Supports SNMP and RMON • Compatible with DMV standard System Management Framework (also OpenView) • In use at DMV
4.	Shomiti Surveyor **Rationale:** • Network probe and analysis tool for TCP/IP-based networks • Supports SNMP and RMON • Compatible with DMV standard System Management Framework (also OpenView) • In use at DMV
5.	IBM NetView **Rationale:** • For use on SNA-based OS/390 systems • Already in use on DMV systems at Teale Data Center
6.	Cisco Secure **Rationale:**

#	
	• Used to support network security administration for Cisco hardware • Supports SNMP and RMON • Compatible with DMV standard System Management Framework (OpenView) • In use at DMV
7.	Visual Networks **Rationale:** • Used for network monitoring of the Frame Relay network • In use at DMV
8.	Network Associates Sniffer and Distributed Sniffer **Rationale:** • Used for low-level network diagnostics • In use at DMV

Tech Watch

- SNMP2

Review Cycle

- 6 Months

Performance Monitoring Tool Sub-Component

Performance management/capacity planning tools perform real-time data collection and analysis for monitoring of hardware and application systems performance and analysis of historical data for proactive management of hardware capacities. These technologies and tools should work in tandem to assess current system performance and to develop capacity plans for future system expansions.

Justification

- Helps monitor and report the effectiveness and efficiency of existing technology investments
- Provides for more proactive technology planning based on changing business requirements
- Pinpoints opportunity for enhanced leverage of existing technology infrastructure
- Identifies potential areas of technology over-utilization and operational interrupts

Standards

#	Performance Monitoring Tools Standards
1.	For TCP/IP-based systems (both those managed by DMV and Teale), select Performance Monitoring Tools that are able to interface with the DMV standard System Management Framework **Rationale:** • Performance monitoring tools should operate within the DMV standard systems management framework, in order to facilitate centralized management while requiring the minimum number of different tools and skill sets, and maximizing the possibility of integration with other tools.
2.	Select and configure Performance Monitoring Tools to enable verification of service level agreements (SLAs). **Rationale:** • SLAs cannot be enforced without supporting performance data.
3.	On SNA-based systems managed by Teale Data Center, coordinate with Teale staff to ensure that DMV standards are met. **Rationale:** • Since Teale-managed systems are not fully under DMV control and must meet Teale requirements in order to be manageable, DMV must actively coordinate with Teale to ensure that DMV business needs are supported.

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the selection of the appropriate product for your environment.

#	Performance Monitoring Tools Products
1.	Concord E-Health **Rationale:** • Used for network performance monitoring • In use at DMV
2.	MegaMon C **Rationale:** • For disk, disk adapter and I/O channel performance monitoring • In use at DMV
3.	Oracle Enterprise Manager **Rationale:** • Used for performance monitoring of Oracle databases and applications • In use at DMV
4.	Netfinity Service Manager **Rationale:** • Used for performance monitoring on platforms running Netfinity • In use at DMV
5.	Visual Networks **Rationale:** • Used for performance monitoring of the Frame Relay network • In use at DMV

Tech Watch

- SLA monitoring at Teale

Review Cycle

- 6 Months

Backup and Recovery Tools Sub-Component

The copying of data, programs, and software files to separate media (tape, disk, etc) for the purposes of having the ability to restore these files in the event of media failure, user error, or a disaster.

Justification

- Ensure the recoverability of the operations of a system in the event of a failure within that same system
- Protect against the loss of data, programs, and software

Standards

#	Backup and Recovery Tools Standards
1.	*No standards are currently specified for this subcomponent.*

Products

At the time of this review, the following product(s) were identified as the leaders in this sub-component area. A single product has not been select as the DMV standard. When a product is needed, please contact a BEAM representative to further assist in the selection of the appropriate product for your environment.

#	Backup and Recovery Tools Products
1.	Tivoli Storage Manager **Rationale:** • Backup solution for IBM platforms • In use at DMV
2.	Compuer Associates ArcServe **Rationale:** • Backup solution for Windows platforms • In use at DMV
3.	Endevor Load/Unload **Rationale:** • Used as backup/recovery solution for mainframe-based software managed by Endevor

#	
	• In use at DMV

Tech Watch

- Strong authentication for job scheduling tools
- BMC Patrol
- Investigate tools and processes for mainframe backups at Teale, and whether they comply with BEAM standards
- Veritas NetBackup (currently under evaluation at DMV for Unix and Windows platforms)

Review Cycle

- 6 Months

Disaster Recovery Sub-Component

Disaster recovery encompasses the use of protective measures such as triage, contingency planning, backup procedures, inventory buildups, and year-end operation slowdowns, to maximize system availability in the event of operational failures or other unforeseen events.

Disaster Recovery Planning Systems organize the disaster recovery planning workflow and provide a centralized repository of disaster recovery information. This enables a more disciplined, standard process to be followed, and makes it more likely that all parts of a disaster recovery plan are addressed during the planning process.

Justification

- Ensure the continued operations of an enterprise in the event of a disaster
- Veritas

Standards

#	Disaster Recovery Planning Tools Standards
1.	*No standards are currently specified for this subcomponent.*

Products

#	Disaster Recovery Planning Tools Products
1.	Living Disaster Recovery Planning System **Rationale:** • Supports Guidelines for this Sub-Component • In use at DMV

Tech Watch

None

Review Cycle

- TBD

Version Control Sub-Component

Please refer to the Version Control Tools Sub-Component in the BEAM Applications Development Component for details.

Revision History

June 26, 2000 – Component Principles version approved at Consensus Meeting.

January 15, 2002 – Products version approved at Consensus Meeting.

November 20, 2002 – Reviewed and approved for BEAM Intranet.